



General Assembly

January Session, 2019

Raised Bill No. 903

LCO No. 4439



Referred to Committee on INSURANCE AND REAL ESTATE

Introduced by:
(INS)

AN ACT CONCERNING INSURANCE DATA AND INFORMATION SECURITY.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. (NEW) (*Effective October 1, 2019*) (a) This section may be
2 cited as the "Insurance Data Security Law".

3 (b) The purpose of this section is to establish standards for data and
4 information security for persons licensed and required to be licensed
5 by the Insurance Commissioner, require licensees to notify the
6 commissioner following cybersecurity events and require the
7 commissioner to investigate such events.

8 (c) As used in this section:

9 (1) "Assuming insurer" means an insurer, including, but not limited
10 to, an insurer that is a licensee, that acquires an insurance obligation or
11 risk from a ceding insurer pursuant to an agreement between the
12 insurers;

13 (2) "Authorized individual" means an individual who is known to,

14 and screened by, a licensee, and to whom the licensee deems it
15 necessary and appropriate to grant access to nonpublic information
16 that is in the possession, custody or control of such licensee or stored
17 on such licensee's information systems;

18 (3) "Ceding insurer" means an insurer, including, but not limited to,
19 an insurer that is a licensee, that transfers an insurance obligation or
20 risk to an assuming insurer pursuant to an agreement between the
21 insurers;

22 (4) "Consumer" means an individual, including, but not limited to,
23 an applicant, beneficiary, certificate holder, claimant, insured or
24 policyholder, who is a resident of this state and whose nonpublic
25 information is in the possession, custody or control of a licensee or
26 stored on a licensee's information systems;

27 (5) "Cybersecurity event" means an event that involves
28 unauthorized access to, or disruption or misuse of, a licensee's or third-
29 party service provider's information systems or the nonpublic
30 information stored thereon, except: (A) An event involving encrypted
31 nonpublic information when the encryption process or encryption key
32 is not acquired, released or used without authorization from the
33 licensee or third-party service provider; or (B) if the licensee or third-
34 party service provider determines that the person who accessed such
35 nonpublic information (i) did not use or release such nonpublic
36 information to a third party, and (ii) destroyed or returned such
37 nonpublic information to such licensee or third-party service provider;

38 (6) "Encryption" means a process that transforms nonpublic
39 information into a form that is unlikely to reveal the meaning of the
40 nonpublic information without the use of a protective process or key;

41 (7) "Information security program" means a comprehensive written
42 program that contains the administrative, physical and technical
43 safeguards that a licensee uses to access, collect, dispose of, distribute,
44 process, protect, store, transmit, use or otherwise handle nonpublic
45 information;

46 (8) "Information system" means: (A) A discrete set of electronic
47 information resources organized for the collection, disposition,
48 dissemination, maintenance, processing, sharing or use of electronic
49 data or information; or (B) a specialized system, including, but not
50 limited to, an environmental control system, industrial or process
51 control system, or a telephone switching and private branch exchange
52 system;

53 (9) "Licensee" means a person that is, or is required to be,
54 authorized, licensed or registered in this state pursuant to title 38a of
55 the general statutes, except: (A) For a purchasing group or risk
56 retention group, as such terms are defined in section 38a-250 of the
57 general statutes, that is chartered and licensed in another state; or (B) if
58 such person is not domiciled in this state and is acting in such person's
59 capacity as an assuming insurer;

60 (10) "Multifactor authentication" means a process that requires an
61 individual to submit not less than two of the following forms of data or
62 information to verify the individual's identity: (A) Information that is
63 within the personal knowledge of such individual, including, but not
64 limited to, a password; (B) electronic data or information that is within
65 the possession, custody or control of such individual, including, but
66 not limited to, a token or text message on a mobile telephone; or (C)
67 data or information inherited by such individual, including, but not
68 limited to, biometric data;

69 (11) "Nonpublic information" means data and information, other
70 than public information and information concerning age or gender: (A)
71 Concerning the business of a licensee that, if accessed, disclosed,
72 tampered with or used without authorization from the licensee, would
73 have a material adverse impact on the business, operations or security
74 of such licensee; (B) that is in a form or medium created or derived
75 from a consumer or health care provider concerning (i) the behavioral,
76 mental or physical health of the consumer or a member of the family of
77 such consumer, (ii) health care provided to the consumer, or (iii)
78 payment for health care provided to the consumer; or (C) concerning a

79 consumer, including, but not limited to, the name, number, personal
80 mark or other personal identifier of the consumer, that, in combination
81 with any of the following forms of information, can be used to identify
82 such consumer: (i) An access or security code, or a password, that
83 would permit access to a financial account; (ii) an account, credit card
84 or debit card number; (iii) biometric records; (iv) a driver's license
85 number or an identification card number; or (v) a Social Security
86 number;

87 (12) "Person" means an individual or a nongovernmental entity,
88 including, but not limited to, a nongovernmental agency, association,
89 branch, corporation or partnership;

90 (13) "Public information" means data or information that: (A) (i)
91 Must be disclosed to the general public pursuant to applicable law, or
92 (ii) may be made available to the general public from government
93 records or widely distributed media; and (B) a licensee reasonably
94 believes, after investigation, (i) is of a type that is available to the
95 general public, and (ii) the consumer has not directed to be withheld
96 from the general public, if the consumer may direct that such data or
97 information be withheld from the general public pursuant to
98 applicable law; and

99 (14) "Third-party service provider" means a person, other than a
100 licensee, that: (A) Contracts with a licensee to maintain, process or
101 store nonpublic information; or (B) is permitted to access nonpublic
102 information while providing services to a licensee.

103 (d) (1) Not later than July 1, 2020, each licensee shall cause a risk
104 assessment program to be implemented for such licensee that:

105 (A) Is continuously operated;

106 (B) Designates an affiliate, employee or outside vendor of such
107 licensee as the person responsible for developing, implementing and
108 maintaining the information security program for such licensee
109 pursuant to subdivision (1) of subsection (e) of this section;

110 (C) Identifies reasonably foreseeable threats, regardless of whether
111 such threats originate inside or outside of such licensee, (i) that might
112 result in unauthorized access to, or unauthorized alteration,
113 destruction, disclosure, misuse or transmission of, nonpublic
114 information that is in the possession, custody or control of such
115 licensee, or (ii) to the security of such licensee's information systems
116 and the nonpublic information that is accessible to, or in the
117 possession, custody or control of, a third-party service provider that
118 has contracted with such licensee;

119 (D) Assesses the likelihood of, and the potential damage resulting
120 from, the reasonably foreseeable threats identified pursuant to
121 subparagraph (C) of this subdivision, taking into account the
122 sensitivity of the nonpublic information described in said
123 subparagraph;

124 (E) Assesses the sufficiency of such licensee's information systems,
125 and all policies, procedures and safeguards implemented to manage
126 the reasonably foreseeable threats identified pursuant to subparagraph
127 (C) of this subdivision, based on an assessment of, among other things,
128 such licensee's policies, procedures and other safeguards concerning
129 threats originating from such licensee's operations regarding (i)
130 employee training and management, (ii) information systems,
131 including, but not limited to, network design, software design and
132 information classification, disposal, governance, processing, storage
133 and transmission, and (iii) detection, prevention and response to
134 cybersecurity events; and

135 (F) Implements information safeguards to (i) manage the reasonably
136 foreseeable threats identified pursuant to subparagraph (C) of this
137 subdivision, and (ii) at least annually, assess the effectiveness of the
138 key controls, procedures and systems comprising such safeguards.

139 (2) Each licensee shall, on the basis of the risk assessment program
140 implemented for such licensee pursuant to subdivision (1) of this
141 subsection:

142 (A) Include cybersecurity risks in such licensee's enterprise risk
143 management process;

144 (B) Remain informed of emerging threats and vulnerabilities;

145 (C) Utilize security measures when sharing data or information that
146 are reasonable in relation to the character of such sharing and the type
147 of data or information shared;

148 (D) Provide all employees of such licensee with cybersecurity
149 awareness training that is updated, on an ongoing basis, to account for
150 all risks identified in such risk assessment program; and

151 (E) Determine whether the security measures set forth in
152 subparagraphs (E)(i) to (E)(xii), inclusive, of this subdivision are
153 appropriate, and, if such licensee determines that such security
154 measures are appropriate, implement such security measures:

155 (i) Access control measures for such licensee's information systems,
156 including, but not limited to, measures that authenticate the identities
157 of, and restrict access to, authorized individuals;

158 (ii) Measures that identify and manage data, devices, facilities,
159 personnel and systems and enable such licensee to achieve such
160 licensee's business purposes in accordance with the relative
161 importance of such purposes to such licensee's business objectives and
162 risk strategy;

163 (iii) Measures that restrict, to authorized individuals, access to
164 physical locations containing nonpublic information;

165 (iv) Measures that protect, by encryption or other means, nonpublic
166 information while such nonpublic information is transmitted over an
167 external network or stored on a laptop computer or other portable
168 computing device, storage device or medium;

169 (v) Secure development measures for software applications
170 developed and utilized by such licensee;

171 (vi) Measures for assessing, evaluating and testing the security of
172 software applications utilized but not developed by such licensee;

173 (vii) Measures to modify such licensee's information systems in
174 accordance with the information security program developed,
175 implemented and maintained for such licensee pursuant to
176 subdivision (1) of subsection (e) of this section;

177 (viii) Effective control measures, including, but not limited to,
178 multifactor authentication, for individuals accessing nonpublic
179 information;

180 (ix) Measures to regularly test and monitor such licensee's
181 information systems and procedures to detect both actual and
182 attempted attacks on, and intrusions into, such licensee's information
183 systems;

184 (x) Measures to include audit trails within the information security
185 program developed, implemented and maintained for such licensee
186 pursuant to subdivision (1) of subsection (e) of this section to (I) detect
187 and respond to cybersecurity events, and (II) reconstruct material
188 financial transactions in a manner that is sufficient to support such
189 licensee's normal operations and obligations;

190 (xi) Measures to protect against damage or destruction to, or loss of,
191 nonpublic information caused by environmental hazards, including,
192 but not limited to, fire and water, other catastrophes or technological
193 failures; and

194 (xii) Measures to dispose of nonpublic information regardless of the
195 format of such nonpublic information.

196 (e) (1) Not later than October 1, 2020, each licensee shall cause an
197 information security program to be developed, implemented and
198 maintained for such licensee that:

199 (A) Is commensurate with the (i) complexity and size of such
200 licensee, (ii) nature and scope of such licensee's activities, including,

201 but not limited to, such licensee's use of third-party service providers,
202 and (iii) sensitivity of the nonpublic information that is used by, or in
203 the possession, custody or control of, such licensee or stored on such
204 licensee's information systems;

205 (B) Is based on the risk assessment program implemented for such
206 licensee pursuant to subdivision (1) of subsection (d) of this section;

207 (C) Is designed to (i) protect against hazards or threats to the (I)
208 integrity and security of such licensee's information systems, and (II)
209 confidentiality and security of the nonpublic information that is in the
210 possession, custody or control of such licensee, and (ii) minimize the
211 likelihood of harm to consumers resulting from any unauthorized
212 access to, or use of, the nonpublic information that is in the possession,
213 custody or control of such licensee;

214 (D) Establishes, and provides for the periodic reevaluation of, a
215 schedule for the retention of the nonpublic information that is used by,
216 or in the possession, custody or control of, such licensee or stored on
217 such licensee's information systems, and a mechanism for the
218 destruction of such nonpublic information when such licensee no
219 longer requires such nonpublic information; and

220 (E) Includes a written incident response plan that (i) is designed to
221 promptly respond to, and recover from, each cybersecurity event that
222 compromises (I) such licensee's information systems, (II) the continued
223 functioning of any aspect of such licensee's business operations, or (III)
224 the availability, confidentiality or integrity of the nonpublic
225 information that is in the possession, custody or control of such
226 licensee, (ii) addresses such licensee's internal processes for responding
227 to cybersecurity events, (iii) sets forth the goals of such plan, (iv)
228 clearly defines the various responsibilities, roles and levels of decision-
229 making authority concerning cybersecurity events, (v) addresses both
230 internal and external communications and information sharing, (vi)
231 identifies requirements for the remediation of any weaknesses
232 identified in such licensee's information systems or the controls

233 associated with such information systems, (vii) provides for the
234 documentation and reporting of cybersecurity events and any
235 activities undertaken in response to cybersecurity events, and (viii)
236 establishes a process to evaluate and, if necessary, revise such plan
237 following each cybersecurity event.

238 (2) Each licensee shall evaluate, monitor and adjust the information
239 security program developed, implemented and maintained for such
240 licensee pursuant to subdivision (1) of this subsection in a manner that
241 is consistent with:

242 (A) Relevant changes in technology;

243 (B) The sensitivity of the nonpublic information that is in the
244 possession, custody or control of such licensee or stored on such
245 licensee's information systems;

246 (C) Threats to the nonpublic information described in subparagraph
247 (B) of this subdivision, regardless of whether such threats originate
248 inside or outside of such licensee;

249 (D) Changes in the arrangement of such licensee's business,
250 including, but not limited to, acquisitions, alliances, joint ventures,
251 mergers and outsourcing; and

252 (E) Changes in such licensee's information systems.

253 (3) (A) If a licensee is governed by a board of directors, such board,
254 or a committee of such board, shall, at a minimum, require the
255 executive management of the licensee, or a person designated by such
256 executive management, to:

257 (i) Cause an information security program to be developed,
258 implemented and maintained for such licensee pursuant to
259 subdivision (1) of this subsection; and

260 (ii) Report, at least annually, to such board concerning (I) the overall
261 status of the information security program developed, implemented

262 and maintained for such licensee pursuant to subdivision (1) of this
263 subsection, and (II) all matters material to such information security
264 program, including, but not limited to, control decisions, cybersecurity
265 events and responses thereto, recommendations for changes to such
266 information security program, the ongoing risk assessment program
267 implemented for such licensee pursuant to subdivision (1) of
268 subsection (d) of this section, risk management measures, testing
269 results and third-party service provider arrangements.

270 (B) If the executive management of a licensee designates a person
271 that is not a member of such executive management to perform the
272 responsibilities established in subparagraph (A) of this subdivision,
273 such executive management shall:

274 (i) Oversee the development, implementation and maintenance by
275 such person of an information security program for such licensee
276 pursuant to subdivision (1) of this subsection; and

277 (ii) Require that such person submit a report, at least annually, to
278 such executive management containing the information set forth in
279 subparagraph (A)(ii) of this subdivision.

280 (4) Not later than October 1, 2021, each licensee shall require each
281 third-party service provider that contracts with such licensee, or is
282 permitted to access nonpublic information that is in the possession,
283 custody or control of such licensee or stored on such licensee's
284 information systems, to implement appropriate administrative,
285 physical and technical measures to protect and secure all information
286 systems that are, and all nonpublic information that is, accessible to or
287 held by such third-party service provider. Each licensee shall exercise
288 due diligence in selecting third-party service providers.

289 (f) Not later than February 15, 2021, and annually thereafter, each
290 insurer domiciled in this state shall submit to the Insurance
291 Commissioner, in a form and manner prescribed by the commissioner,
292 a written statement certifying that such insurer is in compliance with
293 the provisions of subsections (d) and (e) of this section. Each insurer

294 domiciled in this state shall maintain, for a period of not less than five
295 years from the date such insurer submits a written statement to the
296 commissioner pursuant to this subsection, all data, information,
297 records and schedules supporting such written statement. If an insurer
298 domiciled in this state identifies areas, processes or systems that
299 require material improvements, redesign or updates, the insurer shall
300 document and identify all remediation efforts, whether such efforts are
301 planned or underway, to address such areas, processes or systems.
302 Each insurer domiciled in this state shall, upon demand by the
303 commissioner, make available to the commissioner all written
304 statements and documents that such insurer is required to maintain
305 pursuant to this subsection.

306 (g) (1) Beginning on October 1, 2020, each third-party service
307 provider that discovers that a cybersecurity event involving such
308 third-party service provider's information systems has occurred shall,
309 in a form and manner prescribed by the Insurance Commissioner and
310 in no event later than seventy-two hours after discovering such
311 cybersecurity event, notify each licensee that has contracted with such
312 third-party service provider and is affected by such cybersecurity
313 event, or each person designated to act on behalf of a licensee, that
314 such cybersecurity event has occurred.

315 (2) (A) Except as provided in subparagraph (B) of this subdivision, if
316 a licensee suspects that a cybersecurity event involving the licensee's
317 information systems has occurred, such licensee, or a person
318 designated to act on behalf of such licensee, shall promptly conduct an
319 investigation to, at a minimum, determine whether the suspected
320 cybersecurity event occurred, and, if the suspected cybersecurity event
321 occurred:

322 (i) Assess the nature and scope of such cybersecurity event;

323 (ii) Identify all nonpublic information that might have been
324 involved in such cybersecurity event; and

325 (iii) Perform, or oversee the implementation of, reasonable measures

326 to (I) restore the security of such information systems, and (II) prevent
327 further unauthorized acquisition, release or use of the nonpublic
328 information that is stored on such information systems.

329 (B) If a third-party service provider notifies a licensee, or a person
330 designated to act on behalf of a licensee, pursuant to subdivision (1) of
331 this subsection that the third-party service provider has discovered
332 that a cybersecurity event involving such third-party service provider's
333 information systems has occurred, or if a licensee has actual
334 knowledge that such a cybersecurity event has occurred, the licensee
335 shall:

336 (i) Confirm, and maintain records confirming, that such third-party
337 service provider promptly conducted an investigation that satisfies the
338 requirements established in subparagraph (A) of this subdivision; or

339 (ii) Promptly conduct an investigation that satisfies the
340 requirements established in subparagraph (A) of this subdivision on
341 behalf of such third-party service provider.

342 (3) (A) Except as provided in subparagraph (B) of this subdivision,
343 each licensee, or a person designated to act on behalf of such licensee,
344 shall promptly notify the commissioner, in a form and manner
345 prescribed by the commissioner and in no event later than the
346 applicable deadline established in subdivision (4) of this subsection,
347 that a cybersecurity event has occurred if:

348 (i) Such licensee is (I) an insurer, as defined in section 38a-1 of the
349 general statutes, that is domiciled in this state, or (II) an insurance
350 producer whose home state, as such terms are defined in section 38a-
351 702a of the general statutes, is this state; or

352 (ii) Such licensee reasonably believes that the nonpublic information
353 involved in such cybersecurity event concerns not less than two
354 hundred fifty consumers, and (I) such licensee is required to send
355 notice concerning such cybersecurity event to any government body,
356 self-regulatory agency or supervisory body pursuant to any applicable

357 federal or state law, or (II) it is reasonably likely that such
358 cybersecurity event will materially harm any consumer or any material
359 part of the normal operations of such licensee.

360 (B) Each licensee acting in such licensee's capacity as an assuming
361 insurer, or a person designated to act on behalf of such licensee, shall
362 promptly notify the commissioner and each ceding insurer affected by
363 a cybersecurity event, in a form and manner prescribed by the
364 commissioner and in no event later than the deadline established in
365 subdivision (4) of this subsection, that a cybersecurity event has
366 occurred if:

367 (i) The cybersecurity event involves nonpublic information that (I)
368 comes into the possession, custody or control of, or involves
369 information systems maintained by, such licensee in such licensee's
370 capacity as an assuming insurer, or (II) is stored on the information
371 systems of a third-party service provider that contracted with such
372 licensee in such licensee's capacity as an assuming insurer;

373 (ii) Such licensee reasonably believes that the criteria established in
374 subparagraph (A)(ii) of this subdivision are satisfied; and

375 (iii) Such licensee does not have a direct contractual relationship
376 with the consumers affected by such cybersecurity event.

377 (4) Each licensee, or person designated to act on behalf of a licensee,
378 that is required to send notice to the commissioner pursuant to
379 subparagraph (A) of subdivision (3) of this subsection, or the
380 commissioner and a ceding insurer pursuant to subparagraph (B) of
381 said subdivision, shall send such notice to the commissioner, or the
382 commissioner and a ceding insurer, as applicable, not later than
383 seventy-two hours after:

384 (A) Such licensee, or the person designated to act on behalf of such
385 licensee, first discovers a cybersecurity event if the cybersecurity event
386 involves information systems maintained by such licensee; or

387 (B) Such licensee, or the person designated to act on behalf of such
388 licensee, receives notice from a third-party service provider pursuant
389 to subdivision (1) of this subsection disclosing that a cybersecurity
390 event has occurred, or such licensee first has actual knowledge that a
391 cybersecurity event involving the information systems maintained by a
392 third-party service provider has occurred.

393 (5) Each licensee, or person designated to act on behalf of such
394 licensee, that notifies the commissioner pursuant to subparagraph (A)
395 of subdivision (3) of this subsection or receives notice from an
396 assuming insurer pursuant to subparagraph (B) of said subdivision
397 shall, not later than the deadline established in subdivision (4) of this
398 subsection and in an electronic form prescribed by the commissioner,
399 submit the following information to the commissioner, if and to the
400 extent that such information is available to such licensee or person,
401 and shall supplement and update such information as additional
402 information becomes available:

403 (A) The date of the cybersecurity event;

404 (B) A description of how the nonpublic information involved in the
405 cybersecurity event was breached, exposed, lost or stolen, including,
406 but not limited to, a description of the specific responsibilities and
407 roles of each third-party service provider involved in the cybersecurity
408 event;

409 (C) How the cybersecurity event was discovered;

410 (D) Whether any nonpublic information involved in the
411 cybersecurity event was recovered and, if such nonpublic information
412 was recovered, how such nonpublic information was recovered;

413 (E) The identity of each person who perpetrated the cybersecurity
414 event;

415 (F) Whether such licensee, or person designated to act on behalf of
416 such licensee, notified any government, law enforcement or regulatory

417 agency, other than the commissioner, regarding the cybersecurity
418 event and, if so, when such licensee, or person designated to act on
419 behalf of such licensee, issued such notice;

420 (G) A description of each specific type of nonpublic information
421 involved in the cybersecurity event, including, but not limited to,
422 financial or medical information;

423 (H) The period during which each information system involved in
424 the cybersecurity event was compromised by such cybersecurity event;

425 (I) The number of consumers affected by the cybersecurity event or,
426 if such number is unavailable, the best estimate of the number of
427 consumers affected by such cybersecurity event;

428 (J) The results of any review conducted by such licensee, or person
429 designated to act on behalf of such licensee, that (i) identifies any lapse
430 in the automated controls or internal procedures of such licensee, or
431 (ii) confirms that all automated controls and internal procedures of
432 such licensee were followed;

433 (K) A description of any efforts undertaken to remediate the
434 conditions that caused or enabled the cybersecurity event;

435 (L) A copy of any privacy policy implemented by or for such
436 licensee;

437 (M) A statement outlining all steps that such licensee, or person
438 designated to act on behalf of such licensee, will take to (i) investigate
439 the cybersecurity event, and (ii) notify all consumers affected by the
440 cybersecurity event;

441 (N) The name of an individual, designated by such licensee or
442 person designated to act on behalf of such licensee, who is (i) familiar
443 with the cybersecurity event, and (ii) authorized to act on behalf of
444 such licensee; and

445 (O) If such licensee is subject to the notice requirement established

446 in subparagraph (A) of subdivision (6) of this subsection, a copy of the
447 notice that such licensee sent to residents of this state, owners and
448 licensees pursuant to section 36a-701b of the general statutes.

449 (6) Each licensee, or person designated to act on behalf of a licensee,
450 that is required to send notice to the commissioner following a
451 cybersecurity event pursuant to subparagraph (A) of subdivision (3) of
452 this subsection, and each ceding insurer who receives notice from an
453 assuming insurer following a cybersecurity event pursuant to
454 subparagraph (B) of said subdivision and maintains a direct
455 contractual relationship with the consumers affected by the
456 cybersecurity event, shall:

457 (A) Notify the consumers affected by the cybersecurity event in the
458 manner specified in section 36a-701b of the general statutes; and

459 (B) If a consumer affected by the cybersecurity event accessed such
460 licensee's services through an insurance producer, as defined in section
461 38a-702a of the general statutes, and such licensee has the current
462 contact information for the insurance producer, notify such insurance
463 producer at a time and in a manner prescribed by the commissioner.

464 (h) Beginning on October 1, 2020, each licensee shall maintain
465 records concerning each cybersecurity event for a period of not less
466 than five years from the date of the cybersecurity event.

467 (i) (1) Beginning on October 1, 2020, whenever the Insurance
468 Commissioner has reason to believe that a licensee has violated any
469 provision of this section, the commissioner shall:

470 (A) Have the power to examine and investigate the affairs of the
471 licensee, in the manner set forth in sections 38a-14 to 38a-16, inclusive,
472 of the general statutes and in compliance with this section, to
473 determine whether such licensee has violated such provision; and

474 (B) Issue and serve upon the licensee a (i) statement setting forth
475 such violation, and (ii) notice of a hearing to be held at a time and

476 place fixed in such notice, which time shall not be less than thirty
477 calendar days after the date of service of such notice.

478 (2) (A) A licensee shall, at the time and place fixed for a hearing in a
479 notice issued and served upon the licensee pursuant to subparagraph
480 (B) of subdivision (1) of this subsection, have an opportunity to be
481 heard and show cause why an order should not be entered by the
482 commissioner (i) enforcing the provisions of this section, or (ii)
483 suspending, revoking or refusing to reissue or renew any license,
484 certificate of registration or authorization to operate the commissioner
485 has issued, or may issue, to such licensee.

486 (B) The commissioner may, after holding a hearing pursuant to
487 subparagraph (A) of this subdivision and in addition to or in lieu of
488 suspending, revoking or refusing to reissue or renew any license,
489 certificate of registration or authorization to operate the commissioner
490 has issued, or may issue, to a licensee, impose on the licensee a civil
491 penalty of not more than fifty thousand dollars for each violation of
492 any provision of this section. The commissioner may bring a civil
493 action to recover the amount of any civil penalty the commissioner
494 imposes on a licensee pursuant to this subparagraph.

495 (3) (A) Except as provided in subparagraph (B) of this subsection:

496 (i) All documents, information and materials that a licensee submits
497 to the commissioner pursuant to subparagraphs (B), (C), (D), (E), (H),
498 (J) and (K) of subdivision (5) of subsection (g) of this section, or that the
499 commissioner obtains in connection with an investigation conducted
500 pursuant to subparagraph (A) of subdivision (1) of this subsection,
501 shall (I) be confidential and privileged, (II) not be subject to disclosure
502 under the Freedom of Information Act, as defined in section 1-200 of
503 the general statutes or any subpoena or discovery in any private cause
504 of action, and (III) not be introduced into evidence in any private cause
505 of action; and

506 (ii) The commissioner and all persons acting on behalf of the
507 commissioner who receive any document, information or material

508 described in subparagraph (A)(i) of this subdivision shall not be
509 permitted or compelled to testify in any private cause of action
510 concerning such document, information or material.

511 (B) The commissioner may:

512 (i) Exercise the commissioner's authority in any legal or regulatory
513 action, or use any document, information and material described in
514 subparagraph (A)(i) of this subdivision in furtherance of such action;

515 (ii) Submit documents, information and materials, including, but
516 not limited to, documents, information and materials described in
517 subparagraph (A)(i) of this subdivision, to the Attorney General, other
518 state, federal or international regulatory agencies and law enforcement
519 authorities, and the National Association of Insurance Commissioners
520 and the affiliates and subsidiaries of such association, provided the
521 recipient of such documents, information and materials agrees, in
522 writing, to maintain such documents, information and materials as
523 confidential in a manner that satisfies the requirements established in
524 subparagraph (A) of this subdivision;

525 (iii) Receive documents, information and materials, including, but
526 not limited to, confidential or privileged documents, information and
527 materials, from the Attorney General, other state, federal or
528 international regulatory agencies and law enforcement authorities, and
529 the National Association of Insurance Commissioners and the affiliates
530 and subsidiaries of such association, provided the commissioner
531 agrees, in writing, to treat such documents, information and materials
532 as if such documents, information and materials were submitted to the
533 commissioner in the manner described in subparagraph (A)(i) of this
534 subdivision;

535 (iv) Submit documents, information and materials described in
536 subparagraph (A)(i) of this subdivision to a third-party consultant or
537 vendor, provided the consultant or vendor agrees, in writing, to treat
538 such documents, information and materials as confidential in a
539 manner that satisfies the requirements of subparagraph (A) of this

540 subdivision;

541 (v) Enter into agreements governing the submission, receipt and use
542 of documents, information and materials in a manner that satisfies the
543 requirements established in this subdivision; and

544 (vi) Notwithstanding any contrary provision in this subdivision,
545 release to any clearinghouse service or database maintained by the
546 National Association of Insurance Commissioners, or any affiliate or
547 subsidiary of such association, a final, adjudicated action that is subject
548 to disclosure under the Freedom of Information Act, as defined in
549 section 1-200 of the general statutes.

550 (C) No waiver of any applicable privilege or claim of confidentiality
551 in any document, information or material shall occur as a result of any
552 submission made to, or receipt by, the commissioner of such
553 document, information or material in the manner described in
554 subparagraphs (A) and (B) of this subdivision.

555 (j) (1) Notwithstanding any contrary provision in this section:

556 (A) Each licensee that has fewer than ten employees or independent
557 contractors shall not be subject to the requirements established in
558 subsections (d) to (f), inclusive, of this section;

559 (B) Each licensee that is subject to the Health Insurance Portability
560 and Accountability Act of 1996, P.L. 104-191, as amended from time to
561 time, and establishes and maintains an information security program
562 that satisfies all applicable provisions of such act and the guidelines,
563 procedures, regulations and rules promulgated thereunder shall be
564 deemed to have satisfied the requirements established in subsections
565 (d) to (f), inclusive, of this section, provided such licensee files with the
566 Insurance Commissioner, in a form and manner prescribed by the
567 commissioner, a certification that such licensee is in compliance with
568 such provisions; and

569 (C) Each licensee that is an agent, designee, employee or

570 representative of any other licensee shall not be subject to the
 571 requirements established in subsections (d) to (f), inclusive, of this
 572 section, and shall not be required to cause an information security
 573 program to be developed, implemented and maintained for such
 574 agent, designee, employee or representative pursuant to subsection (e)
 575 of this section, provided such agent, designee, employee or
 576 representative is covered by the information security program
 577 developed, implemented and maintained for such other licensee.

578 (2) Each licensee that ceases to qualify for an exception under
 579 subdivision (1) of this subsection shall comply with all provisions of
 580 this section that apply to such licensee not later than one hundred
 581 eighty days after such licensee no longer qualifies for such exception.

582 (k) Nothing in this section shall be construed to create a private
 583 right of action, or to affect or limit a private right of action that exists
 584 without regard to this section.

585 (l) The Insurance Commissioner may adopt such regulations, in
 586 accordance with chapter 54 of the general statutes, to implement the
 587 provisions of this section.

588 Sec. 2. Subparagraph (B) of subdivision (2) of subsection (b) of
 589 section 36a-701b of the general statutes is repealed and the following is
 590 substituted in lieu thereof (*Effective October 1, 2020*):

591 (B) The person who conducts business in this state, and who, in the
 592 ordinary course of such person's business, owns or licenses
 593 computerized data that includes personal information, shall offer to
 594 each resident whose [personal] nonpublic information under
 595 subparagraph [(A)] (C)(v) of subdivision [(4)] (11) of subsection [(a)] (c)
 596 of section [38a-999b] 1 of this act or personal information as defined in
 597 subparagraph (A) of subdivision (2) of subsection (a) of this section
 598 was breached or is reasonably believed to have been breached,
 599 appropriate identity theft prevention services and, if applicable,
 600 identity theft mitigation services. Such service or services shall be
 601 provided at no cost to such resident for a period of not less than

602 twenty-four months. Such person shall provide all information
603 necessary for such resident to enroll in such service or services and
604 shall include information on how such resident can place a credit
605 freeze on such resident's credit file.

606 Sec. 3. Section 38a-999b of the general statutes is repealed. (*Effective*
607 *October 1, 2020*)

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>October 1, 2019</i>	New section
Sec. 2	<i>October 1, 2020</i>	36a-701b(b)(2)(B)
Sec. 3	<i>October 1, 2020</i>	Repealer section

Statement of Purpose:

To revise the standards governing (1) insurance data and information security, (2) notices following cybersecurity events, and (3) investigations of cybersecurity events.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]